

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-50422

(43)公開日 平成9年(1997)2月18日

(51) Int. Cl. <sup>6</sup>	識別記号	序内整理番号	F I	技術表示箇所	
G 0 6 F	15/00	3 3 0	9364-5L	G 0 6 F	15/00
	12/00	5 4 7	7623-5B		12/00
	13/00	3 5 1	9460-5E		13/00
		3 5 5	9460-5E		3 5 5

審査請求 未請求 請求項の数 2 O L (全 9 頁)

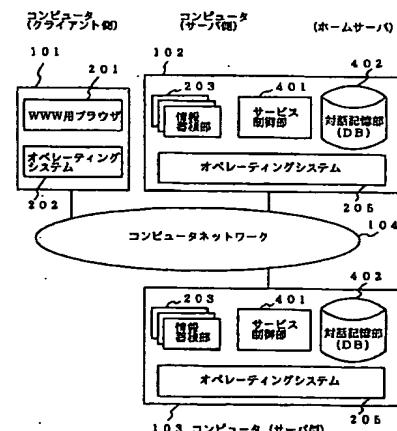
(21)出願番号	特願平7-200107	(71)出願人	000004226 日本電信電話株式会社 東京都新宿区西新宿三丁目19番2号
(22)出願日	平成7年(1995)8月4日	(72)発明者	斎藤 典明 東京都千代田区内幸町1丁目1番6号 日本 電信電話株式会社内
		(72)発明者	水澤 純一 東京都千代田区内幸町1丁目1番6号 日本 電信電話株式会社内
		(74)代理人	弁理士 鈴木 誠

(54) 【発明の名称】コンピュータネットワーク上の対話継承型アクセス制御方法及びそのサーバコンピュータ

(57) **【要約】**

【課題】 コンピュータネットワーク上の複数サーバをまたがった一連のアクセスにおいて、一貫性を持ったアクセス制御を可能にする。

【解決手段】 クライアント 101 とサーバ 102, 103 はネットワーク 104 によって接続される。102 は 101 を用いているユーザのユーザ情報を管理しているホームサーバであり、103 は 101 のユーザ情報を管理していないサーバである。101 はユーザからの URL に従い、102 や 103 に情報取得要求を発行する。102 や 103 は情報取得要求中の対話 ID を解析し、同一ユーザの識別、一連のアクセスの記憶、アクセスのチェックを行う。そして、必要なら他のサーバへ問い合わせて、他のサーバ発行の対話 ID も有効にする。



## Best Available Copy

## 【特許請求の範囲】

【請求項1】 情報提供用のWorld-Wide Webを有するサーバコンピュータとWorld-Wide Webからの情報取得のためのブラウザを有するクライアントコンピュータを含むコンピュータネットワークにおけるサーバ側のアクセス制御方法であって、

クライアント側からの情報取得要求受信時、初回の情報取得要求か、第2回目以降の情報取得要求かを判定し、初回の情報取得の場合は、ID取得要求付き情報要求をもつ初期画面のハイパーテキストをクライアント側に返送し、

第2回目以降の情報取得要求の時、IDの取得要求があり情報提供条件を満たしたユーザからの要求であった場合には、発行元サーバの明記された対話IDを生成し、該対話IDを対話記憶部に登録し、該対話IDを付加したハイパーテキストをクライアントに側に返送し、

ID取得要求でない情報取得要求の場合は、情報取得要求内の対話IDを抽出し、該対話IDから判明する発行元サーバに問い合わせを行い、該発行元サーバからのユーザ認証の結果に基づき情報提供の可否の判定を行い、対話IDが存在しない場合、または正規の対話IDでない場合、または、正規の対話IDでもユーザの属性により情報提供を認めない場合には、アクセス拒否を行うことを特徴とするコンピュータネットワーク上の対話継承型アクセス制御方法。

【請求項2】 コンピュータネットワークで接続したクライアントコンピュータに対し、World-Wide Webの情報をHyper Transfer Protocolにより提供するサーバコンピュータにおいて、同一ユーザからの一連のアクセスを識別する対話識別手段と、同一ユーザのアクセスの履歴を記憶する対話記憶手段と、アクセス履歴を複数サーバから参照する事により情報提供を制御する制御手段を有することを特徴とするサーバコンピュータ。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、コンピュータネットワーク上の対話継承型アクセス制御方法及びそのサーバコンピュータに関し、詳しくは、ハイパーテキストをコンピュータネットワーク上でユーザに提供するための通信サービスのアクセス制御に関するものである。

## 【0002】

【従来の技術】 従来、ハイパーテキストをコンピュータネットワーク上で、ユーザに対して提供する通信サービスとしてWWW(World-Wide Web)が知られており、そのための方法としてHTTP(Hyper Text Transfer Protocol)がある。この方法は、不特定多数のユーザへのサービス提供を行うものであるが、従来はユーザのハイパーテキストに対する一連の操作に対して情報取得の要求が生じた時のみ、情報取得要求中のプロト

コル、IPアドレス(サーバアドレス)、ポート番号、取得する情報等を設定したURL(Uniform Resource Locator)で指定されるサービス提供元のサーバに接続を行い情報の取得を行っている。

【0003】 図7は、この従来のWWWのシステム構成を示したものである。同図において、101はサービスの提供を受けるためにユーザが用いるコンピュータ(クライアント側コンピュータ)、103はサービスを提供するためのコンピュータ(サーバ側コンピュータ)で、

10 両者はネットワーク104によって接続されている。コンピュータ101の内部において、201がWWWサービスの提供を受けるための各種ブラウザ、202が該コンピュータ101を制御するための各種オペレーティングシステムであり、また、コンピュータ103の内部において、203がWWWサービスにおいてユーザに提供するための情報(ハイパーテキストなど)の蓄積部、204がWWWサービスを提供するための各種デーモン、205が該コンピュータ103を制御するための各種オペレーティングシステムである。ブラウザ201では、20 コンピュータの入力装置から入力されたユーザからのURLに従い、ネットワーク上のWWWサーバに情報取得要求を発行する。情報取得要求を受けたWWWサーバのデーモン204では、URLで示される情報蓄積部203内の情報をユーザに転送する。

【0004】 図8に、この従来のWWWサーバのサービス提供シーケンスの一例を示す。同図において、複数のユーザから複数回情報提供要求がある場合でも同様の手順で情報を返送する。

【0005】 上記従来のWWWにおけるHTTPは、不30 特定多数のユーザへの通信サービスが対象であり、一連の情報取得要求の中から同一ユーザの識別、ユーザごとの操作履歴の記憶、アクセス履歴により情報の保護を行えない。

【0006】 これに対して、先に本出願人は、一連の情報取得要求の中から同一ユーザの識別、ユーザごとの操作履歴の記憶、アクセス履歴による情報の保護を行う機能を拡張した方式を提案した(特願平7-125387号「対話管理型情報提供方法及び装置」)。

【0007】 図9は、特願平7-125387号のシステム構成を示したものである。101、103及び104は図7と同様である。クライアント側コンピュータ101の内部において、201がWWWサービスの提供を受けるための各種ブラウザ、202が該コンピュータ101を制御するための各種オペレーティングシステムであり、また、サーバ側コンピュータ103の内部において、203がWWWサービスにおいてユーザに提供するための情報(ハイパーテキストなど)の蓄積部、401が対話管理可能なWWWサービスを提供するためのデーモン、402が対話管理を行うために必要な情報を蓄積する対話記憶部、205が該コンピュータを制御するた

めの各種オペレーティングシステムである。ブラウザ201からは、コンピュータの入力装置から入力されたユーザからのURLに従い、ネットワーク上のWWWサーバに情報取得要求が発行される。情報取得要求を受けたWWWサーバのデーモン401では、対話記憶部402の情報をもとにWWWサービスの提供の可否を判定し、サービス提供を許可する場合にはURLで示される情報蓄積部203内の情報をユーザに転送する。

【0008】図10に、この場合のクライアントとサーバ間のシーケンスの一例を示す。ここで、一連のアクセスを対話と呼ぶことにする。ユーザからのアクセスの初期の段階において、サーバがその対話に対する識別子(対話ID)を生成し、次のアクセスに必要となるURLにその対話IDを付加したハイパーテキストをユーザに提供する。クライアントからは、転送してきたハイパーテキスト上の所定の文字をユーザがクリックすることにより、対話ID付きURLによってサーバにアクセスを行う。

【0009】上記特願平7-125387号の方式では、不特定多数のユーザを対象とした通信サービスにおいて高度がアクセス制御が可能であるが、これらの機能の有効範囲はそれぞれの情報提供元のサーバに対してのみである。このため、WWWを用いた一連の情報取得において、コンピュータネットワーク上の様々な情報提供サーバ間をまたがってアクセスする場合、それぞれのサーバにおいて別々に情報取得要求の認証を行う必要が生じる。

#### 【0010】

【発明が解決しようとする課題】本発明の目的は、ハイパーテキストをコンピュータネットワーク上で、不特定多数のユーザに提供するWWWを用いた通信サービスにおいて、一連の情報取得要求の中から同一ユーザの識別、ユーザごとの操作履歴の記憶、アクセス履歴による情報の保護等の高度なアクセス制御を可能にすると同時に、複数のサーバをまたがった一連のアクセスにおいても一貫性を持ったアクセス制御を可能にして、それぞれのサーバでの別々の情報取得要求の認証を不要にすることにある。

#### 【0011】

【課題を解決するための手段】本発明は、WWWにおけるHTTPで利用されるURLに先の特願平7-125387号で導入した同一ユーザからの一連の情報を識別する識別子(対話ID)を、コンピュータネットワーク上に多数存在するサーバ間で継承して管理する事を最も重要な特徴とする。

#### 【0012】

【作用】本発明では、ユーザからのアクセスの初期の段階において、サーバがその対話に対する識別子(対話ID)を生成し、次のアクセスに必要となるURLと対話IDを付加したハイパーテキストをユーザに提供す

る。クライアントからは、転送してきたハイパーテキスト上の所定の文字をユーザがクリックすることにより、対話IDとURLによってサーバにアクセスを行う。サーバはクライアントから送信された情報取得要求中の対話IDを解析し、同一ユーザの識別、一連のアクセスの記憶、所定のアクセスのチェックなどを行う。これらのチェックにおいて、自サーバ内の対話IDの管理情報による識別だけでなく、他のサーバで管理されている対話IDについても該当のサーバへの問合せを行い、他のサーバ発行の対話IDも有効にする。これにより、サーバをまたがった一連のアクセスにおいても、一貫性を持ったアクセス制御ができるようになる。

#### 【0013】

【実施例】以下、本発明について図面を参照して説明する。

【0014】図1は、本発明を適用するコンピュータネットワークの一実施例を示したものである。同図において、101はサービスの提供を受けるためにユーザが用いるコンピュータ(クライアント側コンピュータ)、102および103はサービスを提供するためのコンピュータ(サーバ側コンピュータ)、104は両者の間で通信サービスを提供するためのネットワークである。クライアント側コンピュータ101では各種のWWW用ブラウザが動作し、サーバ側コンピュータ102および103ではWWWサービスを提供する各種デーモンプログラムが動作し、ネットワーク104を通してユーザに提供するための情報が蓄積されている。102と103の違いは、102は101の側のユーザ情報を管理しており、103は101の側のユーザ情報を管理していない事である。各コンピュータ101、102および103はネットワーク104によって接続されている。

【0015】図2に、本発明のより詳細なシステム構成の一実施例を示す。同図において、クライアント側コンピュータ101中の、201がWWWサービスの提供を受けるための各種ブラウザ、202が該コンピュータ101を制御するための各種オペレーティングシステムであり、また、サーバ側コンピュータ102および103中の、203がWWWサービスにおいてユーザに提供するための情報(ハイパーテキストなど)の蓄積部、40

1が対話管理可能なWWWサービスを提供するためのサービス制御部(デーモン)、402が対話管理を行うために必要な情報を蓄積する対話記憶部、205が該コンピュータ102、103を制御するための各種オペレーティングシステムである。コンピュータ102は、クライアント側コンピュータ101を用いるユーザのユーザ情報を管理しているホームサーバであり、コンピュータ103はクライアント側コンピュータ101のホームサーバではないサーバコンピュータである。

【0016】図3は、コンピュータ102、103内のサービス制御部(デーモン)401の詳細構成を示した

もので、601がアクセス制御部、602が対話識別部、603が通信処理部である。

【0017】クライアント側コンピュータ101のブラウザ201からは、該コンピュータ101の入力装置から入力されたユーザからのURLに従い、ネットワーク104上のWWWサーバに情報取得要求が発行される。

情報取得要求を受けたサーバ側コンピュータ102または103のサービス制御部401では、アクセス制御部601において情報提供およびアクセスの可否の判定を行い、対話識別部602においてはアクセスが許可されたユーザへの対話IDの発行および対話IDごとにユーザのアクセス情報の管理を行い、通信処理部603によって蓄積装置203内の情報をユーザに転送する。

【0018】図4は、本発明によるクライアントとサーバ間のシーケンスの一例を示したものである。ここで、サーバAとサーバBは提携関係にあるとする。

【0019】始めのユーザAに対する例では、クライアント（ブラウザ）においてユーザAからのURLの入力によりサーバAへ情報取得要求（1回目のアクセス）を行い、対話ID取得要求付き初期画面を取得する。次にクライアントでは、ユーザAの操作により対話ID取得要求付き情報取得要求（2回目のアクセス）をサーバAへ行う。サーバAはクライアントからの情報取得要求が情報提供条件を満たしていれば（例えば、ユーザ名とパスワードの一一致などで、この例ではユーザAの情報がサーバAにおいて管理されている）、対話IDを発行し、対話記憶部402に対話IDを記憶し、ユーザからの要求のあったハイパーテキスト（これには次の情報取得要求が付いている）に対話IDを付加して出力する。この例では、次の情報取得要求の宛先がサーバB内のハイパーテキストであり、サーバAで発行された対話IDが付加された情報取得要求をサーバBに発行する（3回目のアクセス）。対話ID付き情報取得要求を受け付けたサーバBは、対話IDを解析し、対話ID発行元のサーバAへ対話IDの照会とユーザ情報の取得要求を発行する。サーバAでは、サーバBからの問合わせに対して、対話記憶部402を検索して対話IDの認証を行い、サーバBへ認証結果およびシステム内（例えばOSへの問合わせ）のユーザ情報を返送する。サーバB、ではサーバAから送信されて来た認証結果およびユーザ情報に基づき、サーバB内の情報のユーザAへの提供の可否を判定する。この例では、ユーザAへの情報提供を認めたため、サーバBは自情報蓄積部203内のハイパーテキストをユーザAに出力する。

【0020】次のサーバBをホームサーバとするユーザBに対する例では、クライアント（ブラウザ）においてユーザBからのURLの入力によりサーバAへ情報取得要求（1回目のアクセス）を行い、対話ID取得要求付き初期画面を取得する。次にクライアントでは、ユーザBの操作により対話ID取得要求付き情報取得要求（2

回目のアクセス）をサーバAへ行う。しかし、この例では、ユーザBの情報がサーバAにおいて管理されておらず、ユーザBは一連のアクセスの過程においてホームサーバにおける認証を行っていない（サーバBが発行した対話IDがない）為に、サーバAにおいてアクセスが拒否される。

【0021】図5は、対話ID付き情報取得要求の実施例の一つとして、対話ID付きURLの一例を示したものである。初期画面を得るための始めのアクセスにおいて用いられる一回目のアクセスのURLは従来のWWWと同様である。2回目のアクセスにおいて、このURLにID取得要求を付加している。3回目以降のアクセスにおいては、各種情報取得要求の他に発行元サーバを明記した対話IDを付加してサーバにアクセスを行う。そして、この対話IDが他のサーバに対しても継承される。

【0022】図6は、サーバ側コンピュータにおけるサービス制御部401の動作のフローチャートを示したものである。図6中、破線で囲った部分がアクセス制御部601と対話識別部602の動作、それ以外は通信処理部603の動作である。

【0023】まず、ステップ1002において、サービス制御部への入力がクライアントからの情報取得要求であるか、他のサーバからの対話IDの問い合わせかを判別する。他のサーバからの対話IDの問い合わせの場合は、ステップ1003～1006の処理を行い、判定結果とユーザ情報を問い合わせのあったサーバへ返送する。クライアントからの情報取得要求である場合は、初回アクセスであるのか、ID取得要求であるのか、対話ID付き情報取得要求であるのか、ステップ1007および1009で判別する。初回アクセスの場合は、ステップ1008でID取得要求付き初期画面を返送するための処理を行う。ID取得要求の場合は、ID取得要求と共に送信されてくるユーザ情報を基づき対話ID発行の可否をステップ1010において判別し、対話ID発行を許可する場合には、ステップ1011～1014の処理を行ってユーザに情報を提供し、許可しない場合は、ステップ1015でアクセス拒否のメッセージを出力する。対話ID付き情報取得要求の場合は、ステップ1016で対話IDの抽出、ステップ1017で該対話IDのチェックを行う。そして、対話IDが自分自身が発行したものである場合は、ステップ1018～1020の処理に従いユーザに情報を提供し、他サーバの発行した対話IDの場合は、ステップ1021で対話IDで識別されるサーバへ対話IDの問い合わせを行い、ステップ1022で判定結果とユーザ情報を取得した後、ステップ1023でアクセスの可否をチェックし、アクセスを許可する場合はステップ1024、1025でユーザに情報を提供し、その以外の対話IDの場合は不正な対話IDとみなし、ステップ1026でアクセス拒否の処理を行う。

## 【0024】

【発明の効果】以上説明したように、本発明によれば先の特願平7-125387号において導入した一連のアクセスに対する識別子を、異なるサーバ間で継承して有効にする事により、サーバにまたがった一連のアクセスにおいて一貫性を持ったアクセス制御ができるようになる。

## 【図面の簡単な説明】

【図1】本発明で対象とする通信サービスを提供するためのシステム構成の一例である。

【図2】本発明によるシステム構成の一実施例の詳細図である。

【図3】図2のサーバ内のサービス制御部の詳細図である。

【図4】本発明におけるクライアントとサーバ間のシーケンスの一例である。

【図5】本発明における対話ID付き情報取得要求を実現するためのURLの一例である。

【図6】本発明におけるサーバのサービス制御部のフローチャートの一例である。

【図7】従来のWWWサービスを提供するためのシステ

ム構成の一例である。

【図8】従来のWWWサービスのサーバとクライアントにおけるシーケンスの一例である。

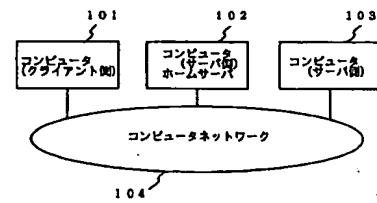
【図9】本出願人が先に提案したシステム構成の一例である。

【図10】図9のシステム構成のサーバとクライアントにおけるシーケンスの一例である。

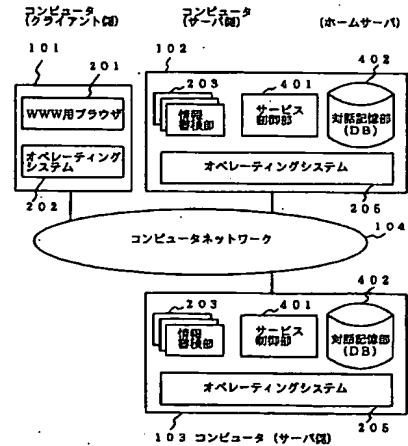
## 【符号の説明】

101 被サービス提供側コンピュータ  
 102, 103 サービス提供側コンピュータ  
 104 ネットワーク  
 201 WWWブラウザ  
 202 オペレーティングシステム  
 203 情報蓄積部  
 204 WWWデーモン  
 205 オペレーティングシステム  
 401 サービス制御部  
 402 対話記憶部  
 601 アクセス制御部  
 602 対話識別部  
 603 通信処理部

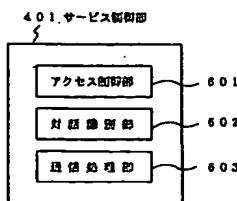
【図1】



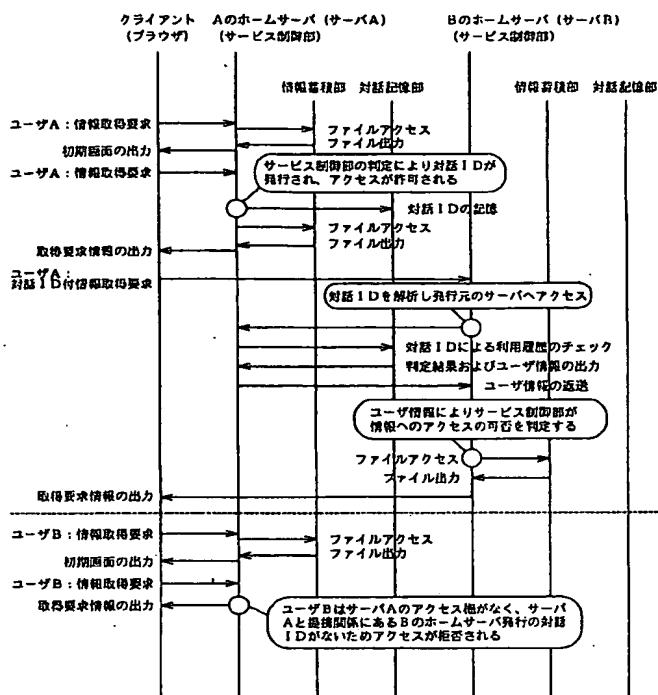
【図2】



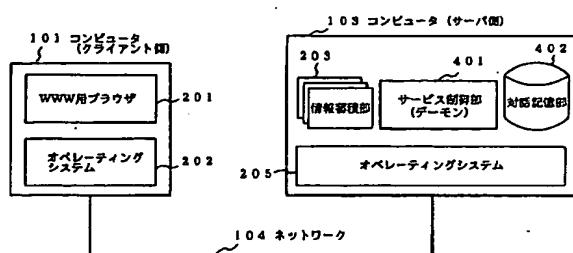
【図3】



[図4]



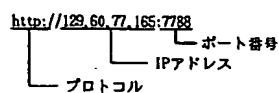
[図9]



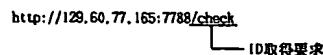
[図5]

## URLの例

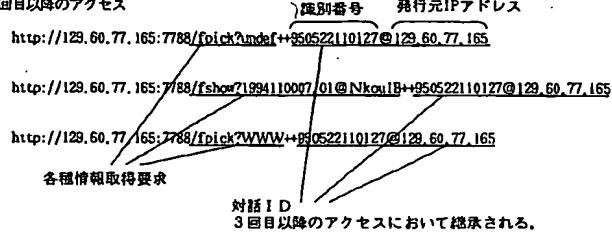
## 1回目のアクセス



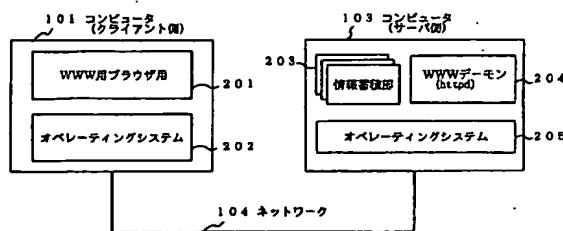
## 2回目のアクセス



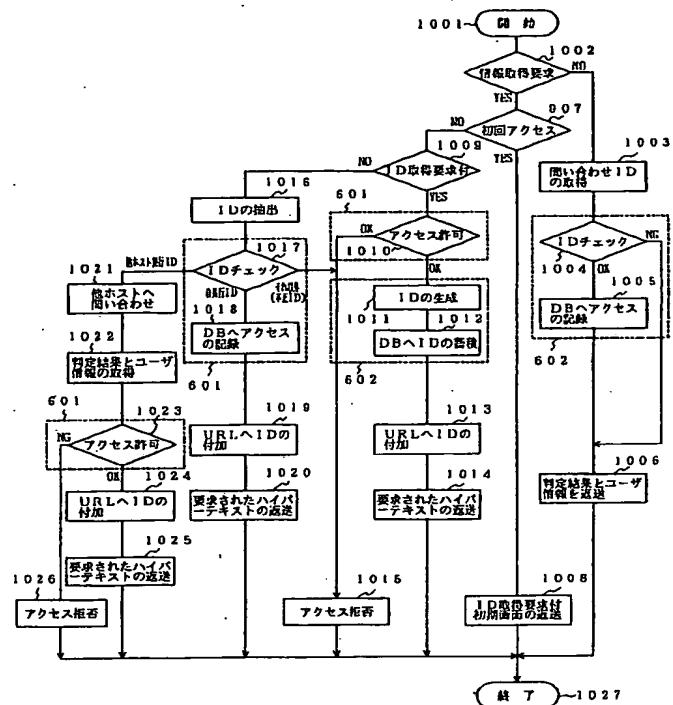
## 3回目以降のアクセス



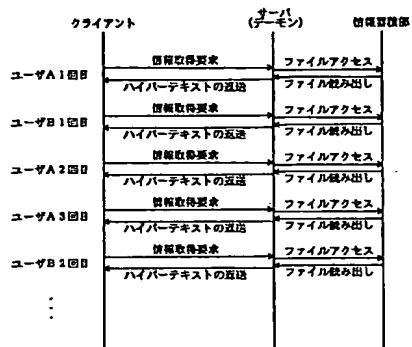
[図7]



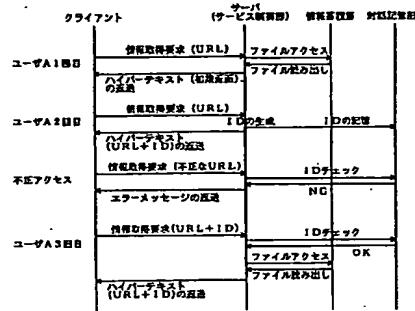
[図6]



【図8】



【図10】



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** Small print

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**